(a1) Let, 'p' be a prime number and 'a' be an integer that not divisible by p, then $a^{p-1} = 1 \pmod{p}$

proof of Fermat's little Theorem:-

Let 'a be such that gcd(a,p) = 1 and considers the set of integers:

$$S = \{1, 2, 3, \dots, p-1\}$$

multiply each element in the set by a modulo p

Since, gcd(a,p)=1, multiplying by a is a bijection in module p, so no two elements a i=aj mod p for $i\neq j$

(ET) let ibipe quilland unipertedang on rett. 9i=1 (a.i) = a [] i p-1 i = ap-1 p-1 i (mod p) 1 = a (mod p) Hence: Feremat's little Theorem is proved sidere the extraction intelleres Example: [1-9 8.5.1] = 8 Griven 1 a=7, + P=13 doos plaitlum i. ged (13, 7) = 1 apply feromatis little 9 pom (7 = 1. (mod 13) 2. 0 = 30 0 2158, 12 mod 13 1=1.1= (919) bog. 55mi? tion in modulo P. so no two elements o. Apply Application in RSA Crzyptography: RSA (Rivest shaming-Adleman) is a public Key-cryptosystem that rulies heavily on

on numbers theory and modulars arithme.

feremat's little Theorem helps in:

(i) Reduces large powers module a prieme during encryption and decryption.

Q2. Prime Factorization of n = 3545100.

:. 3545 100 = 22x33.52 13.101

Eulers's Totient Function formula:

if, n = pk, pke, ... pm

then, $\phi(n) = n \cdot \prod_{i=1}^{m} \left(1 - \frac{1}{P_i}\right)$

So, p(3545100) = 3545100. (1-1/2). (1-1/3). (1-1/5)

 $= 3545100. \frac{1.2.4.12.100}{2.3.5.13.101}$

=> 1.2.4.12.100 =9600

```
2.3.5.13.101 = 39390
     : · p (3545100) = 864864
      ini caled methent elleAmsignmons!
i) les duces large poweres modulo o pr
   Q3. Given Congruinces:

x = 2 mod 3
        2=3 mod 4
022 Prime Paciforisate Dora 1 = x35 45100.
   Let, m, = 30, m2=4; m3=5001 2128 ...
    N= 3.4.5 = 60
Survey to tot or solver solver
   :. X = a, M, y, +a, M, y2 + a, M, y3 mod N
            n = PK, PE ... Pm
       a, = 2, a2 = 35 a3 = 1
  50, q(354510) = 3545300. (1-12). (1-13).
     Ji= Mi! mod m;
  = 3545100. 1.2.4.12.100
   => 1.2.4.12.100 =9600
```

Compute Milodman De Milomoso &

Mi =
$$\frac{66}{30}$$
 = 20

Mi = $\frac{66}{30}$ = 20

Mi = $\frac{66}{30}$ = 20

$$M_2 = \frac{66}{4} = 15$$

Mow, 111.

Q4. A Caremichael numbers is a composite numbers in such that for all integers a with ged (ain) = 1 it satisfies.

an-1 = 1 (modn) 00

prime factorization of 561

561 = 3×11×17 = 156 20. 91 = 1 mod 3 = 57 = 5

Now, 15.12 = 1 mod

3-1=2|560

12= 3

11-1 = 10 | 560

17-1 = 16/560 Bbom 1 = et's1

All three satisfy the condition.

x = 2.20.2 + 3.15.3 + 1.12.3 mod 60 So, 561 is a caronichate number. = 80+135+36 = 251 mod 60

: 251 mod 60 = 11

X = 11 mod GO

Qs. A numbers of is a preimitive root module 17 Orca17(9)=16

That is gk \$1 mod 17 for all K<16 but g16=1

gd # 1 mod 17 forc all prime divisors

(Anh.)

channel.

we must check:

98 ≠1 mod 17

24 ≠ + mod 177 81= 15 Forit Day

92 \$1 mod 17

Mow, g = 3 (let)
map to cycliq militaryol stability ent 10

or 3 =9 modily 7 + 1710 site of elem

34 = 81 mod 17 = 13 # 1 haide lasolara

38 = 13 = 16 mod 17 = 16 #1010

Finally, 36 mod 17 = 1.

So, 9 = 3 passes all the tests.

Q6. Let's Compute 32 mod 17 forex = 1 to 16

 $\frac{3^{2} \mod 18}{1}$ $\frac{2}{1}$ $\frac{2}{$

QR. The discrete logarithm plays a centra role in the Diffie-Hellman key Exchange protocol, which allows two pareties to securely share a secret key overs a publichannel.

1 = 11 bon 18. [1]

The role of the Discrete Logarithm: security of Diffle-Hellman rulies on difficulty of the Discrete Logarithm Given gip and A = ga mod p, find, a Mechinim Replace letters Heartrang This is computationally hard fore large priemes, and there is no efficient algorithm known to solve it in general. This makes it infesible for an eaves -Medium Harulet drappers to determine the sharted secre Example HELLO > KHOOR HEITO PIEHTO LIHETTO!

18. Comparcison among substitution ciphers.
Transposition ciphers, playfaire ciphers. Given bellow.

and the second second second	Serbstition Cipher		playfair cipher
Mechraism	Replace letters	Rearcroing	Replace
		letter	Letterc pairs
Key space		Depends on perconutation	25.
		Preserved	Disquised
fruquency Attack	elerumine the	Medium b of 27999	Harder
Example	HELLO > KHOOR	HEMO > LEHPO	HELLOSCEPP

Q9. a) Encrypt the plaintext "Dept of ICT, MB-stu"

plaintext: DEPTOFICT MBSTU.

Convert letters to numbers

Letterz	pos	Apply (5x+8) mod 26	Cip
D	3	$(5\times3+8) = 23$	×
docks at 4.	d otni	574+8= 28>2	C
all a post of moits	n 15	5×15+8=83>5	Y
		197635× 1948>> 7810	A
property to		substitution:	
	20	(05)U= 1+(0)T (x)5x-20 +8=188->4	F
U		S(18) +2 = \text{\tin}\text{\tett{\text{\te}\tint{\texi}\text{\text{\text{\text{\text{\text{\text{\texi}\tiex{\text{\ti}\tilit{\text{\ti}\text{\text{\text{\text{\text{\text{\texi}\	
. Ca the final	Ciph	entext:	
Hamber VI	XC	FZAHWSZQNUZE	
HADD XIA	ono C-T	- Her Contract Carlotte	

:. First Expheretest Louis !

Q10. Encryption process:

step1: Substitution (shift Based on PRNG)

Tradext: DEPTOFICT MOST (i) Gunerrate a pseudo-random shift-value using a speedmen of 2019/19/ 3010/10)

8-667 (2548 with step 2: permutation

(i) Group text into blocks of 4.

(ii) Apply fixed permutation patteren [3,1,4,2]

Example: TESTCIPHER

Substitution:

T(19)+1 = U(20)

P-P(4)+30=+(7)

S(18) + 2 = U(20)

T(19) +4 = x (23)

ייXטHUזיי (

· Permutation [3.1,4,2] > UHUX > UUXH

:. Final cipheratext [UUXH]